An investigation of improvement of liveness model checking performance degraded by obese formulas

1630011 KOYANAGI Satoshi

Keywords fairness, liveness property, Maude, model checking, divide & conquer approach

In the report, we reproduce the claim that the following technique is effective: the divide & conquer approach to liveness model checking under fairness assumptions. We have conducted two case studies in which it was model checked that two mutual exclusion protocols, Qlock protocol and TAS protocol, enjoy the lockout freedom property under fairness assumptions with and without the approach. Qlock is a mutual exclusion protocol that uses an atomic queue and can be regarded as an abstract version of the Dijkstra binary semaphore; TAS is a mutual exclusion protocol that uses a test & set atomic instruction. An informal description of the lockout freedom property is that whenever each process wants to enter the critical section, it will be eventually there. Qlock and TAS used in the project do not enjoy the property if we do not use any fairness assumptions. The approach was mainly proposed by Ogata [1,2,3]. We have confirmed the effectiveness of the approach through the two case studies. We also summarize some possible improvements in the approach that have been found through the case studies.

Model checking is one of the powerful techniques that verify highly important systems, such as concurrent systems, circuit designs, and communication protocols. Besides, it is one of the most significant achievements in computer science. Model checking is not merely one research topic in computer science but also daily used in industries, especially hardware ones.

We sometimes need fairness assumptions in model checking of liveness properties. Fairness is an abstraction of process scheduling of operating systems that treat all processes fairly. One possible way to use fairness assumptions is to embed them in a temporal formula to model check as the premise of an implication. This makes a temporal formula obese. Because it is time-consuming to convert temporal formulas into Büchi automata, it often becomes impossible to conduct liveness model checking under fairness assumptions with this approach.

Some techniques have been proposed to make it feasible and efficient to model check liveness properties under fairness assumptions. The divide &

conquer approach to liveness model checking under fairness assumptions is one such technique. The technique divides a temporal formula into multiple smaller formulas such that the conjunction of the multiple smaller formulas logically implies the original formula for a system under model checking and each smaller formula can be tackled by an existing ordinary model checker. Compared with other existing techniques for liveness model checking under fairness assumptions, it is not necessary to rely on any tools dedicated to the technique but essentially sufficient to use any existing linear temporal logic (LTL) model checker. We have used the Maude (version 2.7.1) LTL model checker in the case studies.

The report consists of 6 chapters. Chapter 1 outlines the background of the project, describes the aim of the project, and mentions the structure of the succeeding chapters. Chapter 2 prepares the preliminaries needed to read the rest of the report, such as Maude, LTL, and fairness assumptions. The divide & conquer approach to liveness model checking under fairness assumptions is described in Chapter 2 as well. Chapters 3 and 4 report on the two case studies, reproducing the claim that the technique is effective. Chapter 5 mentions two model checkers, Process Analysis Tool (PAT) and the Maude Fair LTLR model checker, where LTLR stands for Linear Temporal Logic of Rewriting, which can natively treat fairness assumptions. We also summarize how PAT [4], the Maude Fair LTLR model checker [5], and some other popular model checkers treat fairness assumptions and make a comparison of the divide & conquer approach to liveness model checking under fairness assumptions with them. Chapter 6 concludes the report. We also mention some future directions in Chapter 6.

References

[1] Kazuhiro Ogata. A divide & conquer approach to liveness model checking under fairness & anti-fairness assumptions. Frontiers Comput. Sci., Vol. 13, No. 1, pp. 51-72, 2019.

[2] Kazuhiro Ogata. Model checking liveness properties under fairness & anti-fairness assumptions. In Pornsiri Muenchaisri and Gregg Rothermel, editors, 20th Asia-Pacific Software Engineering Conference, APSEC 2013, Ratchathewi, Bangkok, Thailand, December 2-5, 2013 - Volume 1, pp. 565-570. IEEE Computer Society, 2013.

[3] Kazuhiro Ogata and Min Zhang. A divide and conquer approach to model checking of liveness properties. In37th Annual IEEE Computer Software and Applications Conference, COMPSAC 2013, Kyoto, Japan, July 22-26, 2013, pp. 648-657. IEEE Computer Society, 2013.

[4] Yuanjie Si, Jun Sun, Yang Liu, Jin Song Dong, Jun Pang, Shao Jie Zhang, and Xiaohu Yang. Model checking with fairness assumptions using PAT. Frontiers Comput. Sci., Vol. 8, No. 1, pp. 1-16, 2014.

[5] Kyungmin Bae and José Meseguer. Model checking linear temporal logic of rewriting formulas under localized fairness. Sci. Comput. Program., Vol. 99, pp. 193-234, 2015.